Math 4460
5/1/23

Recall:

Gaussian integers

$$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$$

norm:

$$N(a+bi) = a^2+b^2$$

$$N(1-2i) = 1^2+(-2)^2 = 5$$

If $z, w \in \mathbb{Z}[i]$, then

$$N(zw) = N(z)N(w)$$

In $\mathbb{Z}$, we say that $u \in \mathbb{Z}$ is a <u>unit</u> if $\frac{1}{u} \in \mathbb{Z}$.

The units of $\mathbb{Z}$ are $1, -1$.

<u>Def:</u> Let $u \in \mathbb{Z}[i]$

We say that u is a <u>unit</u> if $\frac{1}{u} \in \mathbb{Z}[i]$.

<u>Ex:</u>

$\frac{1}{1} = 1 \in \mathbb{Z}[i]$ so $\boxed{1 \text{ is a unit.}}$

$\frac{1}{-1} = -1 \in \mathbb{Z}[i]$ so $\boxed{-1 \text{ is a unit.}}$

$$\frac{1}{i} = \left(\frac{1}{i}\right)\left(\frac{-i}{-i}\right) = \frac{-i}{-i^2} = \frac{-i}{-(-1)} = -i \in \mathbb{Z}[i]$$

so $\boxed{i \text{ is a unit.}}$

$\frac{1}{-i} = i \in \mathbb{Z}[i]$ so $\boxed{-i \text{ is a unit.}}$

So, $1, -1, i, -i$ are units.

Theorem: Let $z \in \mathbb{Z}[i]$.

Then, z is a unit if and only if $N(z) = 1$.

The only units are $1, -1, i, -i$.

proof:

($\Rightarrow$) Suppose z is a unit.

Then, $w = \frac{1}{z}$ is in $\mathbb{Z}[i]$.

So, $zw = 1$.

Hence, $N(zw) = \underbrace{N(1)}_{1 = 1 + 0i}$

So, $N(z)N(w) = 1^2 + 0^2$

Ergo, $\underbrace{N(z)}\underbrace{N(w)} = 1$.

these are regular non-negative integers.

We must have $N(z) = 1$ and $N(w) = 1$.

So, $N(z) = 1$.

$(\Leftarrow)$ Suppose $N(z) = 1$.

Let $z = a + bi$ where $a, b \in \mathbb{Z}$.

Then, $\underbrace{a^2 + b^2}_{N(z)} = 1$.

The possibilities are

$(a,b) = (1,0), (-1,0), (0,1), (0,-1)$

These correspond to

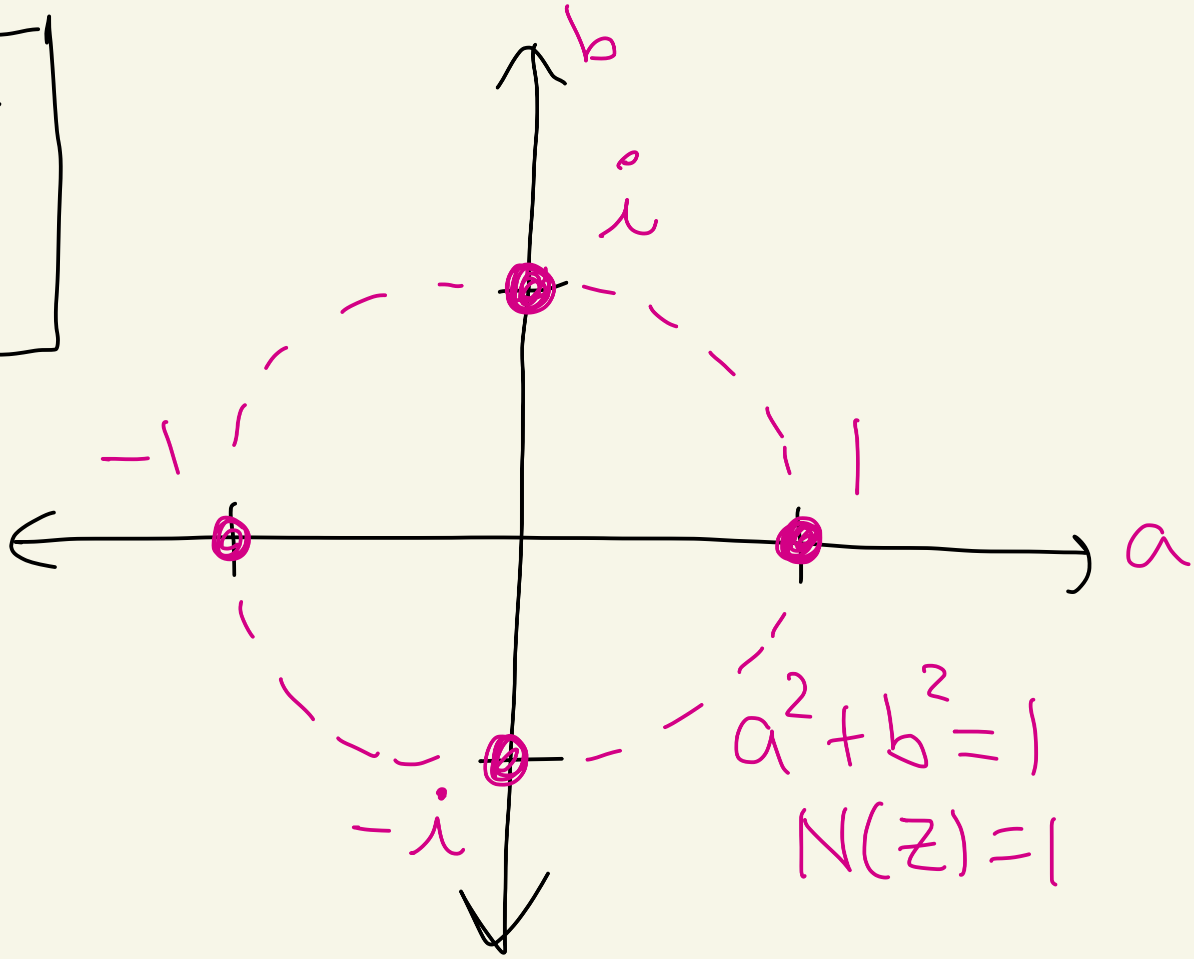
$z = 1, -1, i, -i$.

We saw earlier these are units.

So, z is a unit.

$\blacksquare$

$\boxed{\text{picture of units}}$



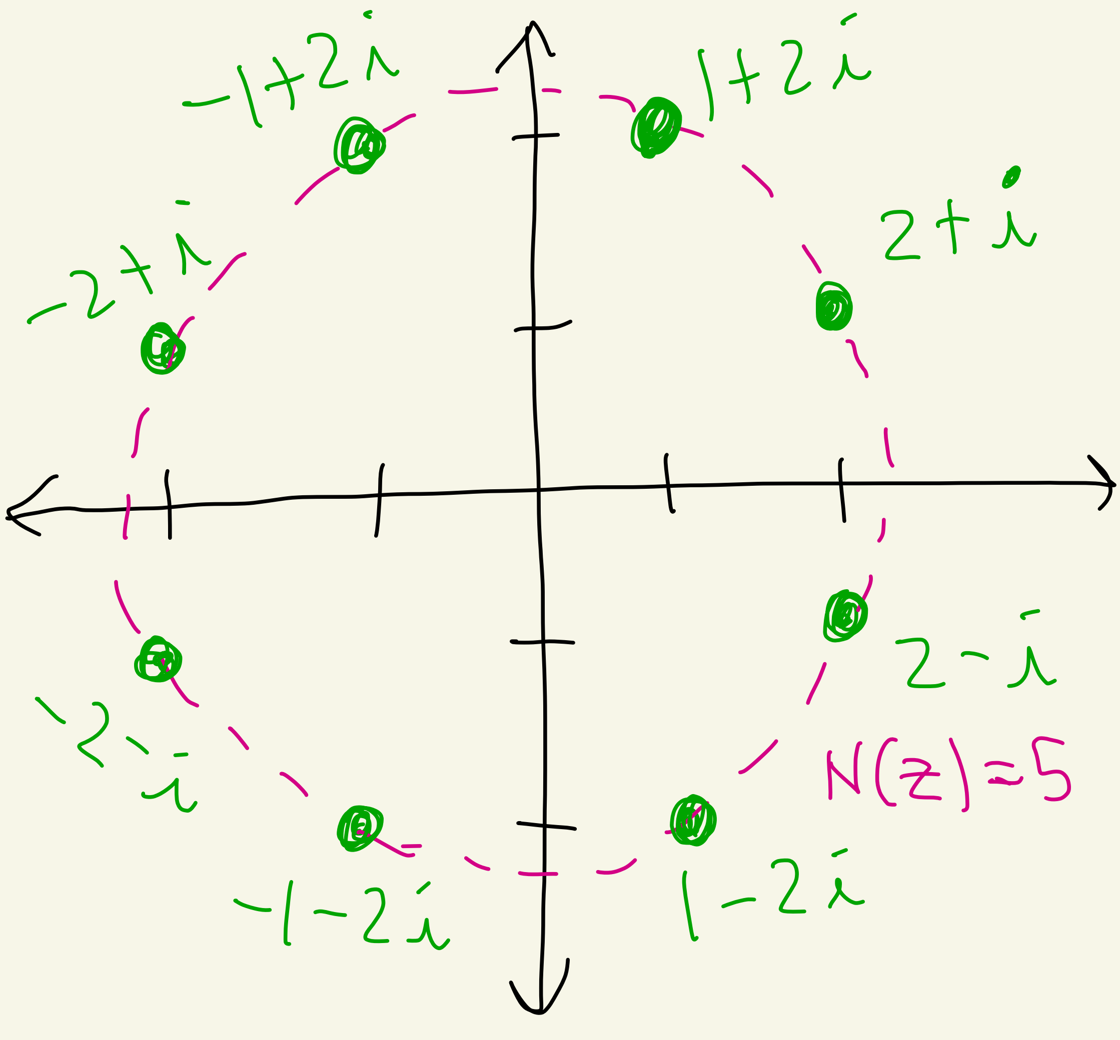
$\boxed{N(z)=5 \text{ picture}}$

$a^2+b^2=5$

circle

center $=0$

radius $=\sqrt{5}$



Def: Let $z, w \in \mathbb{Z}[i]$, $z \neq 0$. We say that z **divides** w if there exists $k \in \mathbb{Z}[i]$ where $w = zk$.

If z divides w, then we write $z \mid w$ and we call z a **divisor** of w.

If z does not divide w then we write $z \nmid w$.

Ex: $3 \mid 6$ since $\underbrace{6}_{w} = \underbrace{3}_{z} \cdot \underbrace{2}_{k}$

$w, z, k \in \mathbb{Z}[i]$

Ex:

$$2 = (1+i)(1-i)$$

So, $(1+i) \mid 2$ and $(1-i) \mid 2$.

Ex: Does $1+i$ divide 3?

Let's see:

$$\frac{3}{1+i} = \frac{3}{1+i} \cdot \frac{1-i}{1-i}$$

$$= \frac{3-3i}{1-\cancel{i}+\cancel{i}-i^2} = \frac{3-3i}{2}$$

$\boxed{i^2 = -1}$

$$= \frac{3}{2} - \frac{3}{2} i \notin \mathbb{Z}[i]$$

So, $1+i$ does not divide 3.

<u>Ex:</u> Find all the divisors of 3.

We have

$$3 = (1)(3)$$
$$3 = (-1)(-3)$$
$$3 = (i)(-3i) \leftarrow (i)(-i) = 1$$
$$3 = (-i)(3i)$$

So, $\boxed{\begin{matrix} 1, -1, i, -i \\ 3, -3, 3i, -3i \end{matrix}}$ ← units

are divisors of 3. Are there more?

Suppose $z \mid 3$ where $z \in \mathbb{Z}[i]$.

Then, $3 = zk$ where $k \in \mathbb{Z}[i]$.

So, $N(3) = N(zk)$.

Thus, $\underbrace{9}_{\substack{3 = 3 + 0i \\ N(3) = 3^2 + 0^2 = 9}} = \underbrace{N(z)}\,\underbrace{N(k)}$

non-negative integers that divide 9.

So, $N(z) = 1, 3,$ or 9.

<u>case 1</u>: Suppose $N(z) = 1$.

Then, by the previous theorem

$\boxed{z = 1, -1, i, \text{ or } -i.}$

We saw these all divide 3.

Case 2: Suppose $N(z)=3$

Let $z=a+bi$, where $a,b\in\mathbb{Z}$.

Then, $a^2+b^2=3$.

a	b	a^2+b^2
0	±1	1
±1	0	1
±1	±1	2
±0	2	$4>3$
$\vdots$	$\vdots$	

all have $a^2+b^2>3$

By the table there are no z with $N(z)=3$.

Case 3: Suppose $N(z)=9$.

Let $z=a+bi$, $a,b\in\mathbb{Z}$.

Then $a^2+b^2=9$.

The solutions are

$$(a,b) = (3,0), (-3,0),$$
$$(0,3), (0,-3)$$

These correspond to
$z = 3, -3, 3i, -3i$

These are the four we found earlier.

Therefore, the only divisors of 3 are $1, -1, i, -i, 3, -3, 3i, -3i$.

$\blacksquare$

Def: Let $z \in \mathbb{Z}[i]$, $z \neq 0$

The elements

$$z, \ -z, \ iz, \ -iz$$

are called the **associates** of z.

Note:

If $z \in \mathbb{Z}[i]$, $z \neq 0$, then

$$\left.\begin{aligned} z &= (1)(z) \\ z &= (-1)(-z) \\ z &= (i)(-iz) \\ z &= (-i)(iz) \end{aligned}\right\}$$

so z is divisible by the units $1, -1, i, -i$ and the associates of z

$z, -z, iz, -iz$

Def: Let $z \in \mathbb{Z}[i]$.

We say that z is <u>prime</u> in $\mathbb{Z}[i]$ if

(1) z is not a unit ← z is not $1, -1, i, -i$

and (2) the only divisors of z are

$$\underbrace{1, -1, i, -i}_{\text{units}}, \underbrace{z, -z, iz, -iz}_{\text{associates of } z}.$$

Ex: We saw earlier that 3 is prime in $\mathbb{Z}[i]$.